SHRegGetPath

The destination string buffer must be long enough to hold the return file path.

Sean Barnum, Cigital, Inc. [vita¹]

Copyright © 2007 Cigital, Inc.

2007-04-16

Part "Original Cigital Coding Rule in XML"

Mime-type: text/xml, size: 4044 bytes

Attack Category	Malicious Inp	out			
		Path spoofing or confusion problem			
Vulnerability Category	Buffer Overf	D 00 0 0			
	Unconditional				
Software Context	File Path Mar	File Path Management			
Location	• shlwapi.h	shlwapi.h			
Description	The destination string buffer for SHRegGetPath() must be long enough to hold the return file path. Otherwise, buffer overflows will occur.				
	SHRegGetPath() retrieves a file path from the registry, expanding environment variables as needed				
APIs	FunctionName		Comm	Comments	
	SHRegGetPath				
	SHRegGetPathA		ASCII	implementation	
	SHRegGetPathW	,	Unicod	le implementation	
Method of Attack	Buffer Overflow	Buffer Overflow			
Exception Criteria					
Solutions		Solution Description		Solution Efficacy	
	is called.	The fourth parameter, pszPath, must be at least MAX_PATH characters in length.		Effective.	
Signature Details	HKEY hkey, LPCTSTR pszSub LPCTSTR pszVal LPTSTR pszPath,	DWORD SHRegGetPath(HKEY hkey, LPCTSTR pszSubkey, LPCTSTR pszValue, LPTSTR pszPath, DWORD dwFlags			

 $^{1. \}quad http://buildsecurityin.us-cert.gov/bsi/about_us/authors/35-BSI.html~(Barnum, Sean)\\$

SHRegGetPath 1

);				
Examples of Incorrect Code	TCHAR pszPath[15 too small	TCHAR pszPath[15]; // Buffer is too small			
	HKEY hkey; [] // set hkey to a handle to a key that is currently open, or a registry root key.				
	<pre>DWORD result = S hkey, TEXT("MySubKey") TEXT("MYValue"), pszPath, 0); if (result != ER handle error */</pre>	, ROR_SUCCESS) { /*			
Examples of Corrected Code	_	TCHAR pszPath[MAX_PATH]; // Buffer is properly sized			
	a key that is cu	<pre>HKEY hkey; [] // set hkey to a handle to a key that is currently open, or a registry root key. DWORD result = SHRegGetPath(hkey, TEXT("MySubKey"), TEXT("MYValue"), pszPath, 0);</pre>			
	hkey, TEXT("MySubKey") TEXT("MYValue"), pszPath, 0				
		<pre>if (result != ERROR_SUCCESS) { /* handle error */ }</pre>			
Source Reference					
Recommended Resources		WISDIN Telefelice for STIREGOETI atti			
Discriminant Set	Operating System	• Windows			
	Languages	• C			
		• C++			

Cigital, Inc. Copyright

Copyright © Cigital, Inc. 2005-2007. Cigital retains copyrights to this material.

Permission to reproduce this document and to prepare derivative works from this document for internal use is granted, provided the copyright and "No Warranty" statements are included with all reproductions and derivative works.

SHRegGetPath 2

For information regarding external or commercial use of copyrighted materials owned by Cigital, including information about "Fair Use," contact Cigital at copyright@cigital.com¹. The Build Security In (BSI) portal is sponsored by the U.S. Department of Homeland Security (DHS), National Cyber Security Division. The Software Engineering Institute (SEI) develops and operates BSI. DHS funding supports the publishing of all site content. 1. mailto:copyright@cigital.com

SHRegGetPath 3